BOJ Reports & Research Papers

金融システムレポート別冊シリーズ

Financial System Report – Annex

サイバーセキュリティに関する金融機関の取り組みと改善に向けたポイント

― アンケート（2017年4月）調査結果 ―

日本銀行
金融機構局

2017年10月

【本レポートに関する照会先】
日本銀行金融機構局考査企画課（csrbcm@boj.or.jp）

（金融システムレポート別冊シリーズについて）

日本銀行は、マクロ・プルーデンスの視点からわが国の金融システムの安定性を評価するとともに、安定確保に向けた課題について関係者とのコミュニケーションを深めることを目的として、『金融システムレポート』を年 2 回公表している。同レポートは、金融システムの包括的な定点観測である。

『金融システムレポート別冊シリーズ』は、特定のテーマや課題に関する掘り下げた分析、追加的な調査等を不定期に行い、『金融システムレポート』を補完するものである。本別冊では、日本銀行が 2017 年 4 月に当座預金取引先金融機関等を対象に実施した「サイバーセキュリティに関するアンケート」の結果を紹介する。

（本別冊の要旨）

金融機関が、IT の進歩に対応し、付加価値の高いサービスを創出していくうえでは、外部などからの攻撃に対する情報の安全管理およびコンピュータシステム・通信ネットワークの安全性や信頼性の確保、すなわちサイバーセキュリティの確保が不可欠である。

日本銀行は、今般、当座預金取引先金融機関等のうち 411 先を対象に、サイバー攻撃の脅威や自社の対策状況などの現状に対する認識、経営資源の割り当てスタンス、実際のリスク管理状況などについて調査するため、アンケートを実施した。この結果、多くの先では、サイバー脅威の認識が深まっており、それに応じて、役員レベルのサイバーセキュリティの責任者を設置し、対策費用も増加させるなど、体制整備に向けた取り組みが進んでいることが確認された。また、技術面でも、脆弱性対策やマルウェア攻撃対策、DDoS 攻撃対策などが相応に進んでいることが確認された。もっとも、個社別にみると、対応状況にはかなりのばらつきがみられた。

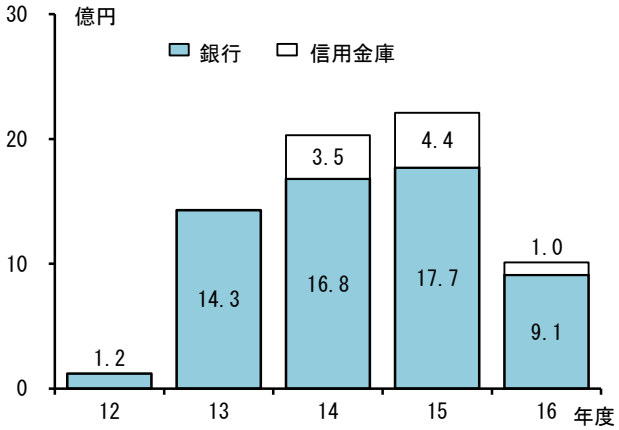
金融機関のサイバーセキュリティ体制については、全ての先に一律の水準が求められるものではない。もっとも、サイバー脅威の高まりを踏まえれば、各金融機関が、対策の強化に不断に取り組みを進めていくことが重要である。日本銀行としては、金融機関が自らのサイバーセキュリティに関する体制面や技術面での取り組みを進めていくうえで、本アンケート結果が活用されることを期待するとともに、金融機関とサイバーセキュリティに関する議論をさらに深めていく方針である。

１．はじめに

最近のわが国の金融機関を取り巻く環境をみると、クラウドサービスやモバイル端末の普及に加え、AI（人工知能）や IoT（Internet of Things）などの技術の進展、FinTech（フィンテック）などの新たなサービスの登場といった大きな変化が生じている。金融機関がこうした環境変化に対応し、付加価値の高いサービスを創出していくうえでは、外部などからの攻撃に対する情報の安全管理およびコンピュータシステム・通信ネットワークの安全性や信頼性の確保、すなわちサイバーセキュリティの確保が不可欠である[1]。

こうした中、最近のわが国の金融セクターを巡るサイバー脅威の状況をみると、インターネット・バンキングを悪用した預金などの不正な引き出しは、2013 年度以降に急増したが、その後はやや落ち着いている（図表 1）。また、これまでのところ、外部からのサイバー攻撃により、わが国の金融機関から大規模な情報漏えいが生じた事例はみられていない。もっとも、わが国全体でみれば、マルウェア[2]やシステムの脆弱性を悪用した攻撃により、大規模な情報漏えいが生じた事例が少なからず発生している（図表 2）。

図表 1　インターネット・バンキングによる預金などの不正引き出し金額の推移



（資料）全国銀行協会、全国信用金庫協会

図表 2　サイバー攻撃に起因した国内の大規模な情報漏えい事例

時期	内容
2013年	不正アクセスによって最大2,200万件の顧客ID情報と100万人強の暗号化されたパスワードが流出した可能性。
2015年	標的型メールによるサイバー攻撃を受け、システムに格納していた100万件強の個人情報が流出。
2016年	子会社職員が、取引先を装った標的型メールの添付ファイルを開きマルウェア感染。不正アクセスにより800万人弱の個人情報が流出した可能性。
2017年	クレジットカードによる支払サイトに不正アクセスが発生し、利用者のクレジットカード情報70万件弱が流出。
2017年	オンラインストアに対して脆弱性を悪用した不正アクセスが発生。100万件超の顧客情報が流出。
2017年	チケットサイトに不正アクセスがあり、個人情報約15万件（うちクレジットカード情報約3万件）が流出。カード不正利用による被害も一部判明。

（資料）各種公表情報

[1] 金融サービスにおける IT の活用とサイバーセキュリティに関する詳細は、『金融システムレポート別冊シリーズ：IT の進歩がもたらす新たな可能性とサイバーセキュリティ』（2016 年 3 月）を参照。

[2] 不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪意のあるコード（コンピュータプログラム）の総称。ウィルス、ワーム、トロイの木馬、スパイウェア、キーロガー、バックドア、ランサムウェアなどが含まれる。

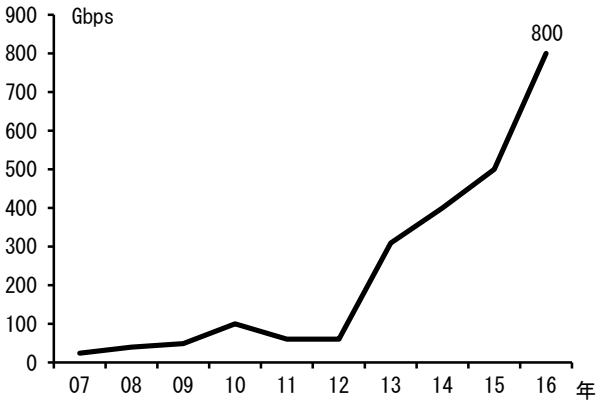
また、海外においては、セキュリティ管理が不十分な金融機関が狙われた不正送金事例や、マルウェアの一種であるランサムウェアにより、感染端末のファイルを暗号化して、その復号の見返りに金銭（身代金）が要求された事例も多数確認されている（図表 3）。この間、DDoS 攻撃[3]は、金融セクターを含む国内外の法人などを対象に、数多く確認されており、攻撃規模も拡大傾向を辿っている（図表 4）。

図表 3　海外の金融機関のサイバー攻撃被害事例

時期	発生国	内容
2013年	韓国	複数の大手金融機関等がマルウェアに感染し、多数のオンライン端末やATMが利用不能化。
2013～2014年	ロシア、米国、ドイツ、中国等	約100の金融機関がマルウェアに感染。不正送金や、ATMからの不正な現金引き出しなどにより、総額1千億円相当以上の被害が発生。
2014年	米国	大手金融機関がマルウェアに感染し、8千万以上の顧客情報が漏えい。
2016年	バングラデシュ	中央銀行のシステムへの不正侵入・情報の窃取が発生。米国にある同行の口座から他国の口座への81百万ドルの不正送金・引き出しが行われた模様。
2016年	ロシア	中央銀行のシステムがサイバー攻撃を受け、同行の口座と商業銀行口座から計20億ルーブル（約31百万ドル）が盗まれた模様。
2017年	ロシア、ウクライナ等	世界中の多数の端末がマルウェア（ランサムウェア）に感染し、業務が不能化。ロシアやウクライナの一部の銀行でも被害が発生した模様。

（資料）各種公表情報

図表 4　DDoS 攻撃の攻撃規模の拡大



（注）Arbor Netwroks が各年で観測した最大値。
（資料）Arbor Networks

このような環境のもと、日本銀行は、今般、当座預金取引先金融機関等のうち 411 先[4]を対象に、サイバー攻撃の脅威や自社の対策状況などの現状に対する認識、経営資源の割り当てスタンス、リスク管理体制の整備状況などを調査することを目的に、サイバーセキュリティに関するアンケート（以下、「アンケート」）を実施した[5]。

アンケート結果をみると、全体として、サイバー脅威に対する金融機関の認識が深まっており、それに応じて体制整備や技術対策も進んでいることが確認できた。もっとも、個社別にみると、対応状況にはかなりのばらつきがみられた。各金融機関のビジネスの内容やインターネットの業務上の利用状況、システム構成、直面するサイバー脅威に違いがあることを

[3] 大量の（または不正な）通信により、標的とするコンピュータや通信回線の機能（サービス）を停止または著しく低下させる攻撃（DoS 攻撃）のうち、インターネット上に分散する複数の機器から同時に攻撃するもの。DoS は Denial of Service、DDoS は Distributed Denial of Service の略。

[4] 内訳は、銀行 124 先、信託銀行 13 先、信用金庫 255 先、系統中央機関 4 先、金融商品取引業者 7 先、証券金融会社 1 先、短資会社 3 先、資金清算機関 1 先、金融商品取引清算機関 2 先、その他 1 先。なお、本稿では、これらの先を総称して「金融機関」という。

[5] アンケート実施期間は、2017 年 4 月 3 日から同 28 日まで。回収率は、100%。

踏まえれば、サイバー攻撃への対応に一律の水準が求められるものではない。しかし、各金融機関は、サイバー脅威の高まりを踏まえ、対策の強化に不断に取り組んでいくことが重要である。日本銀行としては、今後、考査・モニタリングやセミナーなどを通じて、金融機関とサイバーセキュリティに関する議論をさらに深めていく方針である。

以下では、アンケート結果を踏まえつつ、サイバーセキュリティを確保するうえで求められる対応のポイントを紹介する。

2．サイバーセキュリティに関するアンケートの結果

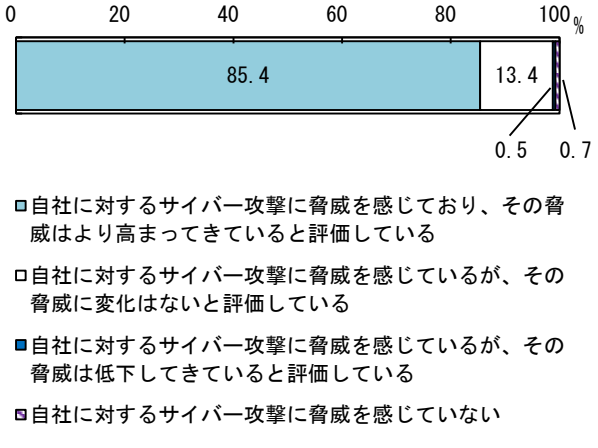
（1）体制面の取り組み

脅威の認識と自社への攻撃の発生状況

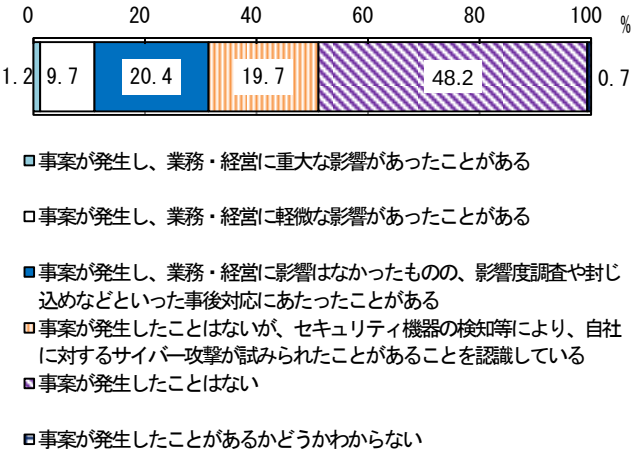
（アンケート結果）

大半の先では、自社に対するサイバー攻撃に脅威を感じており、2015 年頃と比較しても、その脅威はより高まっていると評価している（図表 5）。この間のサイバー攻撃事案の発生状況をみると、業務・経営に何らかの影響のある事案が発生した先（1 割強）、事案が発生し、影響はなかったものの、事後対応にあたったことのある先（約 2 割）、事案は発生しなかったものの、攻撃が試みられたことがあることを認識している先（約 2 割）が、少なからず存在している。これらを合計すると、全体の半数を超える金融機関が、実際に、サイバー攻撃を受けているということになる（図表 6）。詳細をみると、規模の大きな先ほど攻撃を受けた経験があるとの回答割合が高い傾向にあるが、サイバー攻撃は信用金庫などの地域金融機関にも広がっていることが確認された。

図表 5　2015 年頃と比較したサイバー攻撃の脅威認識



図表 6　2015 年以降のサイバー攻撃事案の発生状況



サイバー脅威の内容を適切に認識することは、サイバーセキュリティを確保する対応の基礎となる。最新の脅威動向や自社への攻撃発生状況を適時に把握することで、攻撃者の目的や攻撃対象、攻撃手法の巧妙化や技術レベルの高まりなどを認識し、自社システムのうち防御が必要な箇所や、対応に必要となるコストの多寡などを判断することが可能となる。

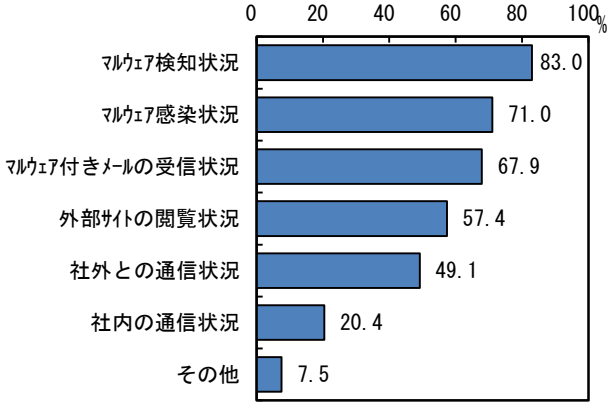
情報の収集・共有

（アンケート結果）

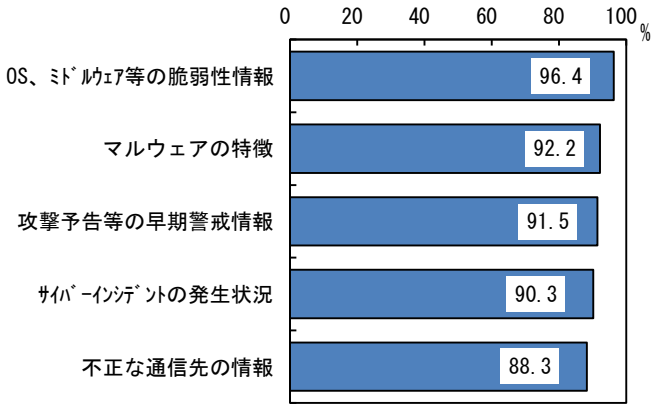
多くの先が、自社システムのマルウェア検知・感染状況や、マルウェア付きインターネットメールの受信状況のモニタリングを行っている（図表 7）。

また、脅威情報についても、OS やミドルウェアの脆弱性、マルウェアの特徴を始め、幅広い情報を収集している（図表 8）。このうち、約半数の先が、脆弱性に関する外部情報を、定期的に収集しているほか、約 4 割の先が、他社で話題になった情報を、その都度収集するとしている（図表 9）。なお、サイバーインシデント（サイバー攻撃によりサイバーセキュリティが脅かされる事案）など、自社が把握した脅威情報を金融 ISAC などの外部機関に発信している先は、全体の 3 割強にとどまっている（図表 10）。

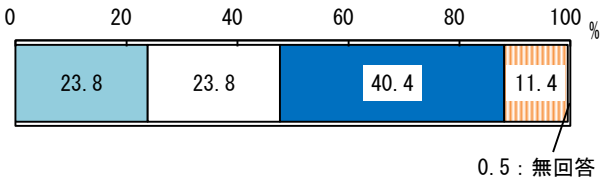
図表 7　自社システムについての
モニタリングの内容（複数回答）



図表 8　収集している脅威情報（複数回答）

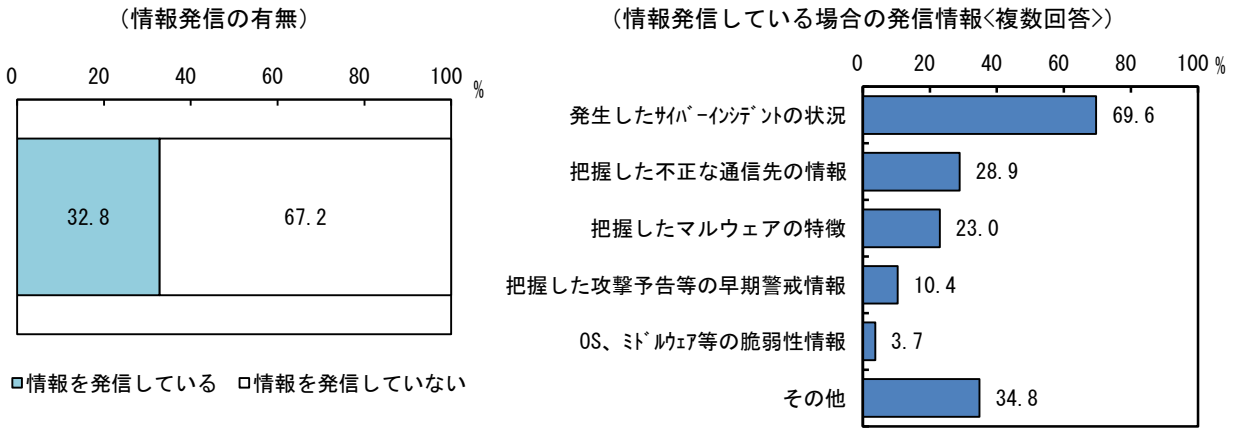


図表 9　脆弱性に関する情報収集



- OS、ミドルウェアの脆弱性情報を機動的かつ定期的に収集し、自社への影響を調査している
- OS、ミドルウェアの脆弱性情報を定期的に収集し、自社への影響を調査している
- 他社で話題になったOS、ミドルウェアの脆弱性情報をその都度収集し、自社への影響を調査している
- 自社では脆弱性情報を収集していない

図表 10　外部機関への情報発信



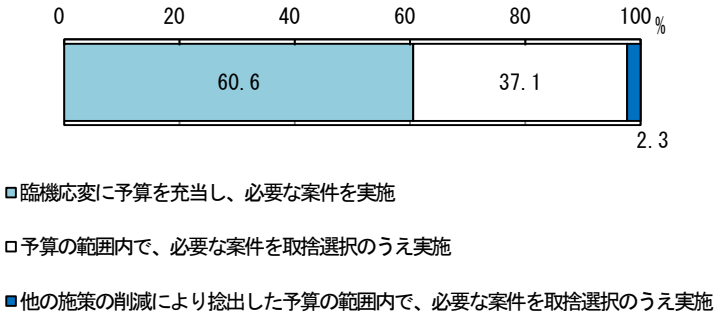
サイバーセキュリティの確保のためには、自社システムへの攻撃やマルウェアの感染状況、通信状況の変化などを適時に把握する必要がある。他者に対して使われた攻撃手法が自らへの攻撃にも使われる可能性があるほか、脅威の内容は時間の経過とともに変化するため、脅威に関する幅広い情報を他者の動向などから収集することは極めて有用である。また、必要に応じて、高度なノウハウを有する外部の専門組織と連携することなども有効な対応になる。他方、社会全体としてサイバーセキュリティを高めていくためには、社会にとって有益な脅威情報を、信頼できる機関などを介して、適時に共有していくことも重要である。

予算・要員の確保

（アンケート結果）

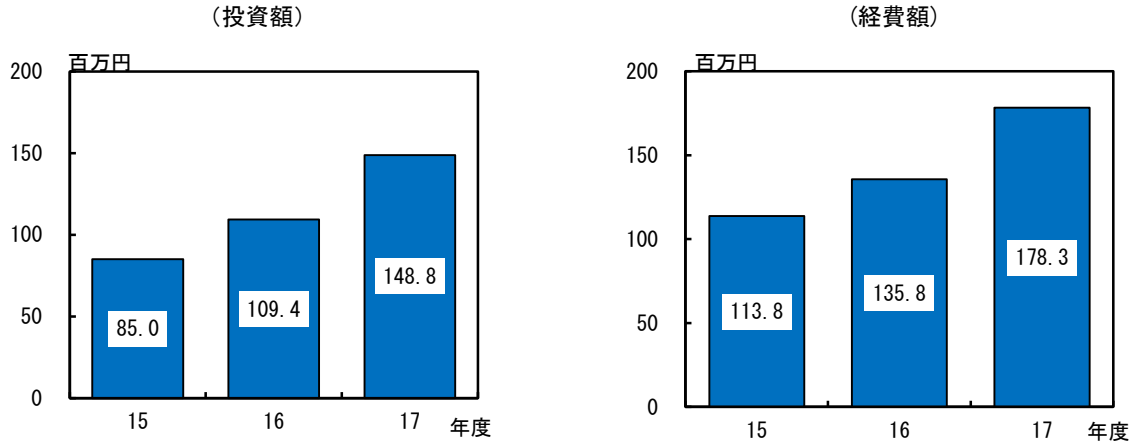
サイバーセキュリティのための投資予算についてみると、約 6 割の先では、必要な施策に対して、臨機応変に予算が充当される状況にある（図表 11）。実際のサイバーセキュリティ関係投資・経費の金額の推移をみても、増加傾向にあることが確認された（図表 12）。

図表 11　サイバーセキュリティのための投資予算の確保



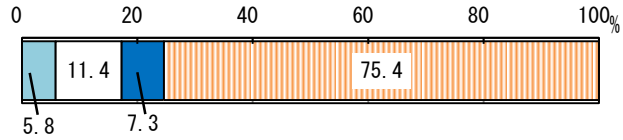
（注）分母は回答があった先数。

図表 12　サイバーセキュリティ関係投資・経費の金額(1 先あたり平均)



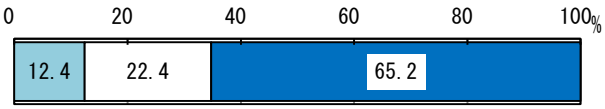
一方で、サイバー攻撃対策にかかるシステム開発・運用に必要なマンパワーを把握し、見直しを行っている先は、全体の 2 割弱にとどまっている（図表 13)。また、サイバー攻撃対策にかかる企画要員については、全体の 6 割を超える先で、「十分に確保できていない」との回答であった（図表 14)。サイバー攻撃対策を整備・推進するうえでの課題をみても、「人材確保・育成」を挙げる先が非常に多い結果となった（図表 15)。

図表 13　サイバー攻撃対策にかかる
人員計画の策定状況



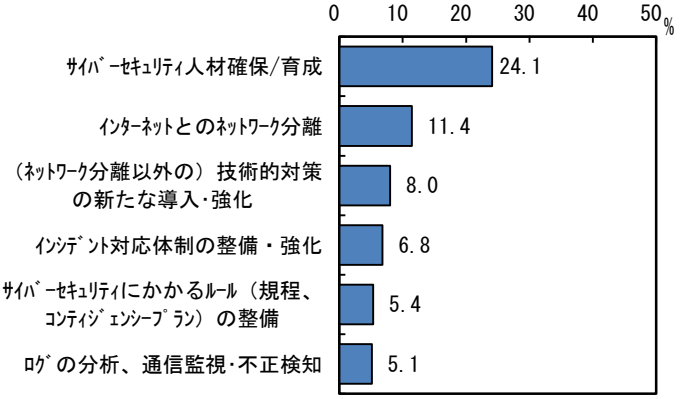
- サイバー攻撃対策にかかるシステム開発・運用の所要マンパワーを把握するとともに、脅威動向に応じ機動的かつ定期的に見直しを行っている
- 所要マンパワーを把握するとともに、定期的に見直しを行っている
- 所要マンパワーを見積もったことがある
- 所要マンパワーを把握していない（IT関連の所要マンパワーと合算しており、サイバー攻撃対策単体では把握していないなど）

図表 14　サイバー攻撃対策にかかる
企画要員の確保状況



- 自社職員のみで要員を十分確保できている
- 自社職員に加え、外部人材の活用により十分な要員を確保できている
- 要員を十分に確保できていない

図表 15　サイバー攻撃対策を整備・推進するうえで認識している課題（自由記述、上位 6 位）



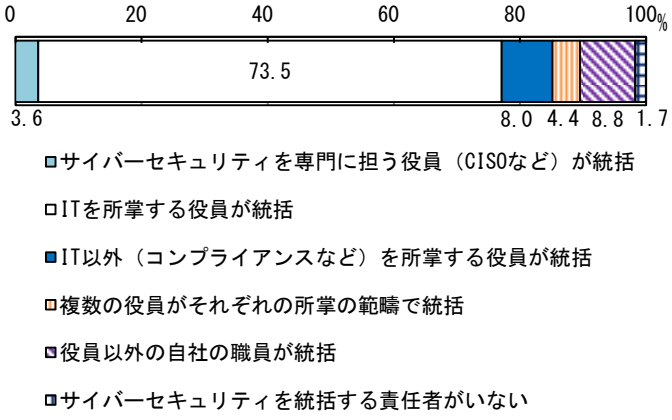
サイバー脅威が高まっている場合、それに応じた対策を講じなければ、サイバーリスク（サイバー攻撃により影響を被るリスク）が増加する。したがって、脅威の高まりに応じて、サイバーリスクを各金融機関が受容可能なレベルに抑制するために必要な投資や、サイバーセキュリティ要員を把握し、その確保に努める必要がある。予算面・人材面での制約への対処には、経営トップの判断が不可欠であるため、セキュリティ担当部署は、経営判断に必要な情報を、適切に報告していくことが重要である。

組織体制

（アンケート結果）

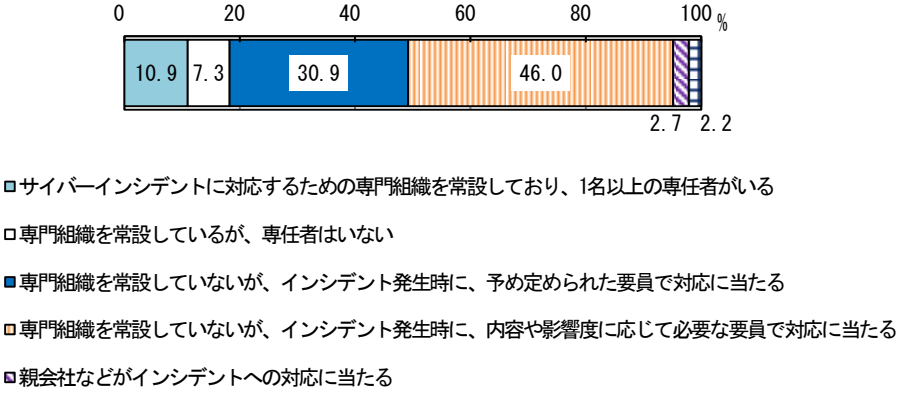
大半の先では、役員レベルの責任者（主として IT を所掌する役員）が自社のサイバーセキュリティを統括している。なお、サイバーセキュリティを専門に担う役員（情報セキュリティ統括責任者＜CISO＞など）を設置済みの先は、現状では少数にとどまっている（図表 16）。

図表 16　サイバーセキュリティを統括する責任者



インシデント対応組織についてみると、1 名以上の専任者を有する組織を常設している先は、全体で 1 割強にとどまり、サイバーインシデント発生時に、予め定められた要員またはインシデントの内容などに応じた要員で対応にあたるとする先が、多数を占めた（図表 17）。

図表 17　サイバーインシデントに対応するための組織の整備状況



高まる脅威に組織的に対応していくうえで、サイバーセキュリティを統括する責任者の存在は欠かせない。サイバー攻撃対応を効果的に進めるためには、強い権限を有する、すなわち役員レベルまたはこれに準じた責任者がその任に当たる必要がある。

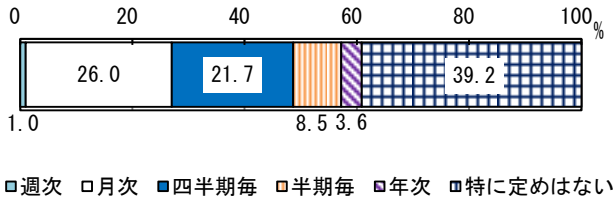
また、攻撃手法が巧妙化する中で、サイバー攻撃を受けた場合に被害が拡大しないよう、即座に対応できる専門部署（インシデント対応組織）[6]を整備する必要がある。インシデント発生時は、サイバー攻撃の影響範囲を早期に把握して対応する必要があるため、対応要員や手順が予め定められていることが望ましい。加えて、サイバー攻撃の発生時以外においても、経営陣への定期報告、関係部署や外部機関との調整、ログの取得・分析や情報収集・共有、体制整備にかかる各種の企画などの対応も期待される。こうした点を踏まえると、インシデント対応組織は、常設組織として設置されていることが望ましい。

経営陣への定期報告

（アンケート結果）

全体の 6 割弱の先では、サイバーインシデントの発生時以外にも、半期に一度以上の頻度で、サイバーセキュリティに関する経営陣への定期的な報告が行われている（図表 18）。

図表 18　サイバーセキュリティに関する経営陣への定期報告の頻度



サイバーセキュリティを確保するうえで、経営陣には、自社のサイバーリスクを把握し、それを踏まえた体制整備に必要な計画の策定や経営資源の投入の要否などの判断が求められる。このため、経営陣に対して、経営判断に必要な情報を定期的に報告する必要がある。また、サイバー脅威やその技術対策、自社のシステム構成などの変化に伴い、サイバーリスクを把握するために必要な情報も変化するため、必要に応じて報告内容を見直すことも重要である。

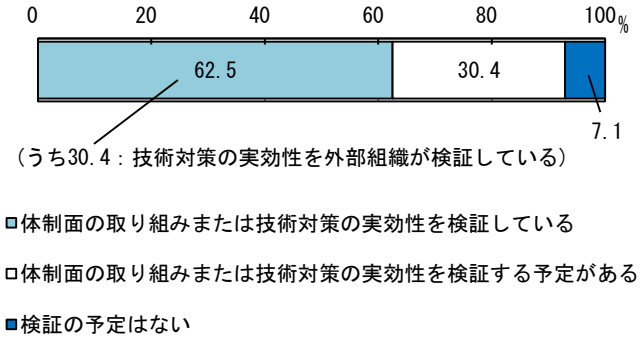
[6] 例えば、CSIRT（Computer Security Incident Response Team）がこれに該当する。

自社の取り組みの実効性の検証

（アンケート結果）

多くの先では、体制面の取り組みや技術対策の実効性について、検証を行っている。ただし、技術対策の実効性を外部組織により検証している先は、3 割程度にとどまっている（図表 19）。

図表 19　サイバーセキュリティに関する体制面の取り組みや技術対策の実効性の検証



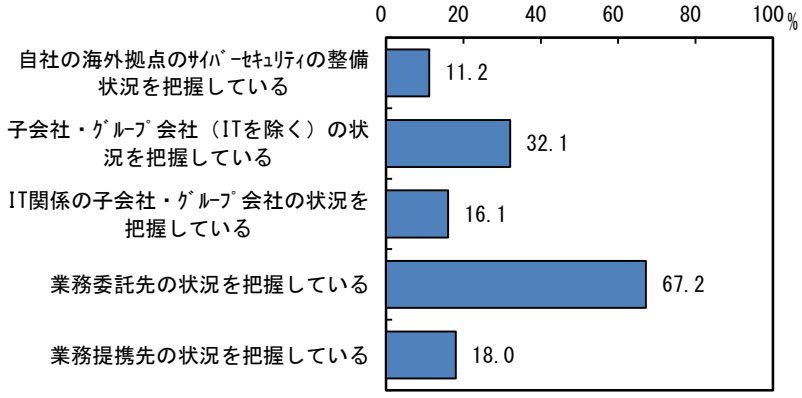
サイバーセキュリティ確保のための体制面の取り組みや技術対策に関しては、その実効性を客観的に検証することが望ましい。特に、技術対策の実効性の検証には、高度な専門性が求められ、自社職員のみで効果的に検証することが困難なケースも想定される。したがって、外部組織による検証を受けることが望ましい。

関連会社などのサイバーセキュリティの整備状況の把握

（アンケート結果）

大多数の金融機関が様々な業務について外部委託を行っている中、全体の 7 割弱の先が業務委託先のセキュリティ整備状況を把握している（図表 20）。

図表 20　関連会社などに対するサイバーセキュリティの管理（複数回答）



（注）分母には、関連会社などを持たない先を含む。

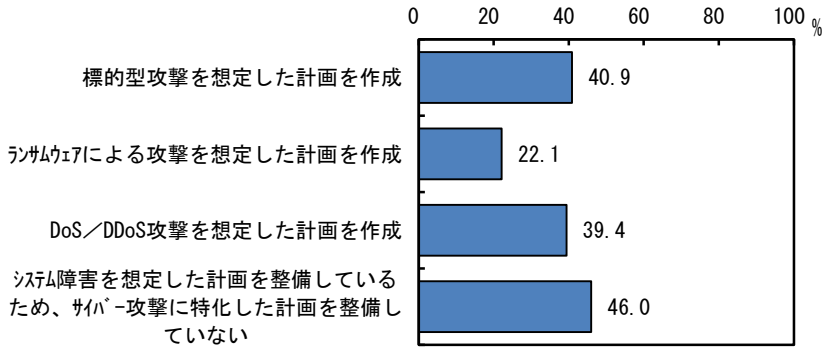
自社の情報資産にアクセスすることが可能な子会社・グループ会社や業務委託先などがある場合には、それらの先のセキュリティ整備状況を把握し、その情報資産の重要性を勘案のうえ、必要な改善を求めていく必要がある。

コンティンジェンシープランの整備

（アンケート結果）

標的型攻撃や DDoS 攻撃を想定したコンティンジェンシープラン（緊急時対応計画）を整備する動きが進んでいる（図表 21）。もっとも、システム障害のコンティンジェンシープランを整備していることから、さらに対応を一歩進めて、サイバー攻撃に特化した計画を整備するには至っていない先が少なくない。

図表 21 コンティンジェンシープランの整備状況（複数回答）



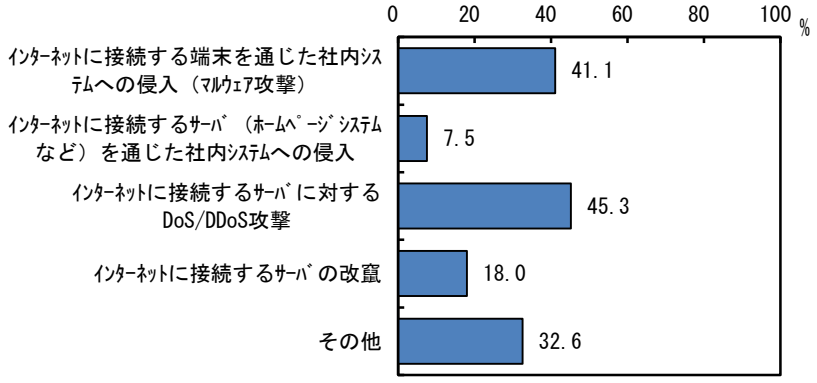
サイバー攻撃の手法が巧妙化する中で、攻撃を防ぎきれない場合に備え、実効性のあるコンティンジェンシープランを整備する必要がある。サイバー攻撃を受けることにより生じる個々の事象には、システム障害が発生した場合の事象との共通点も少なくない。しかし、サイバー攻撃には攻撃者が存在し、2 次攻撃や感染の拡大が生じることから、求められる対応が連続的に発生したり、被害の拡大を防止するために通信の遮断やシステムの停止を行う必要が生じるなど、システム障害時の対応とは異なる点が多い。このため、システム障害の場合とは別のコンティンジェンシープランを整備したり、システム障害用のコンティンジェンシープランを援用しつつ、サイバー攻撃特有の対応を洗い出し、明確化しておくことも必要である。

訓練・演習の実施

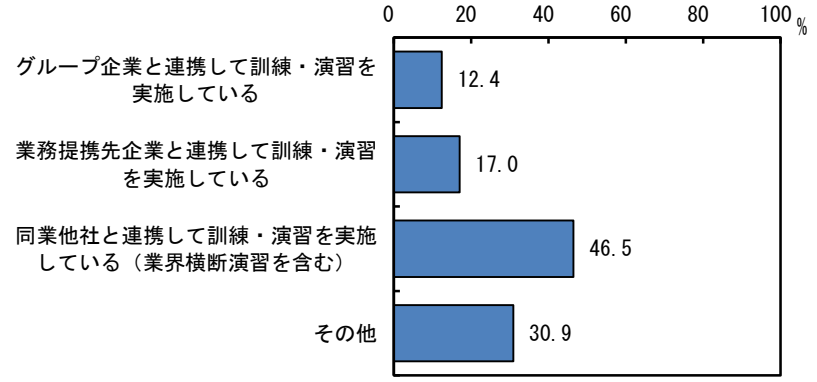
（アンケート結果）

ホームページシステムなど、インターネットに接続するサーバに対する DoS 攻撃（DDoS 攻撃を含む）や、インターネットに接続する端末を通じたマルウェア攻撃を想定した訓練・演習[7]については、それぞれ全体の 4 割を超える先が実施している（図表 22）。また、同業他社と連携して訓練・演習（業界横断演習を含む）を実施している先は、全体の半数弱に達している（図表 23）。

図表 22　実施したことのある訓練・演習の想定シナリオ（複数回答）



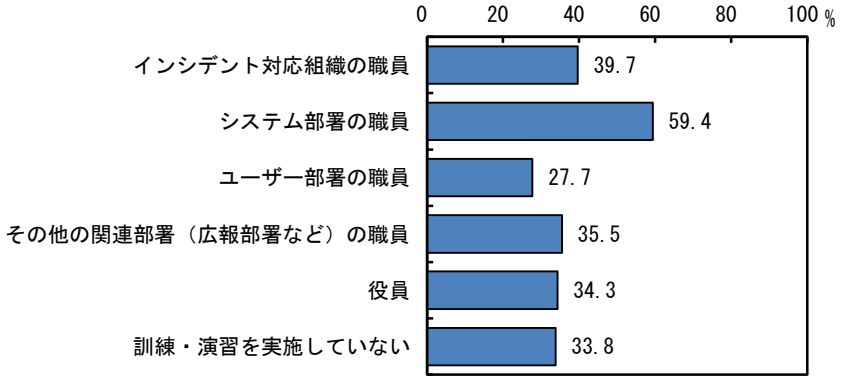
図表 23　訓練・演習での他社との連携状況（複数回答）



訓練・演習の対象者をみると、システム部署の職員を対象にした訓練・演習は、約 6 割の先が実施している。一方で、幅広く役員やユーザー部署の職員を対象にした訓練・演習の実施先は、3 割前後にとどまっている（図表 24）。

[7] 本アンケートでは、既に幅広く実施されている、「標的型攻撃メール受信時の対応確認訓練」を除くベースで質問した。

図表 24　訓練・演習の対象者（複数回答）



自社がサイバー攻撃を受けた際の対応体制について、その機能度を確認するとともに、必要な改善に繋げていくためには、サイバー脅威の種類や強度に応じて、インシデントが発生した場合などを想定した訓練または演習を行う必要がある。多くの場合、サイバー攻撃の影響が及ぶ範囲は、システム部署にとどまらない。このため、システム部署以外の部署の職員も、訓練や演習の対象に含めることが望ましい。また、影響によっては、重大な経営判断や対外公表が必要となることから、役員も対象に含めることが望ましい。

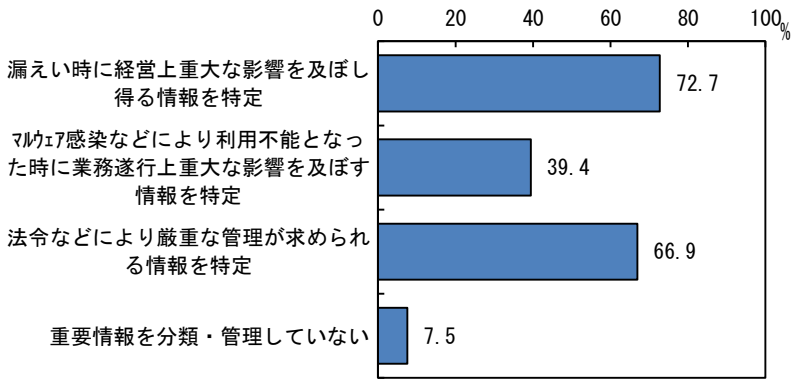
（２）技術面の取り組み

守るべき情報資産の洗い出し

（アンケート結果）

全体の 7 割前後の先が、漏えい時に経営上重大な影響を及ぼし得る情報や、法令などにより厳重な管理が求められる情報を特定している。一方で、マルウェア感染などにより利用不能となった場合に業務遂行上重大な影響を及ぼす情報を特定している先は、約 4 割にとどまっている（図表 25）。

図表 25　重要情報の特定（複数回答）



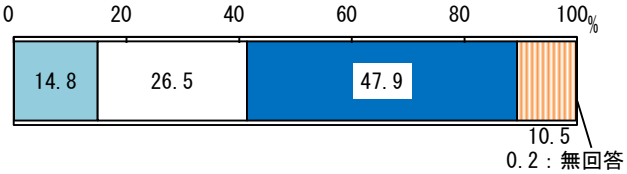
サイバー攻撃の脅威の高まりを踏まえ、攻撃を受けることを前提に、自社が守らなければならない情報資産を予め特定しておく必要がある。その際、サイバー攻撃により生じ得る自社への影響として、情報資産の種類毎に、情報が漏えいするリスク、情報を業務で利用できなくなるリスク、情報の正確性が失われるリスクなどを想定しておく必要がある。そして、その想定の結果を踏まえ、守るべき情報資産を特定し、対応策を講じることが必要である。

重要システムの構成情報の管理

（アンケート結果）

重要なシステムの構成情報[8]を定期的に収集・管理している先は、全体では 4 割強にとどまった。また、重要なシステムの構成情報を管理していないとの回答も、約 1 割の先でみられた（図表 26）。

図表 26　重要なシステムの構成情報の管理状況



脆弱性に関するリスクを管理するうえで、自社のシステムの仕様や構成にかかる情報を定期的に収集し、管理する必要がある。これにより、新たに判明した脆弱性情報について、自社システムへの影響の有無や程度などを迅速に確認・判断することが可能となる。

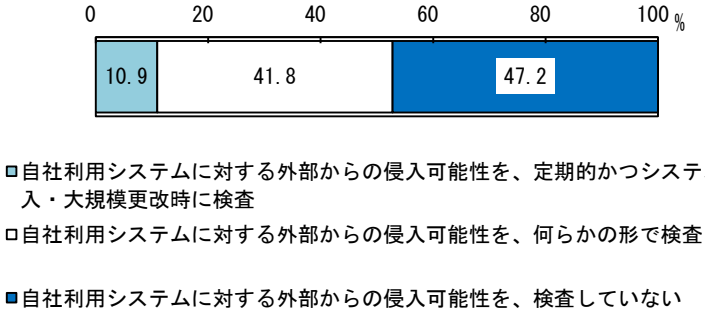
脆弱性検査の実施

（アンケート結果）

過半の先が、何らかの形で脆弱性検査を実施している。大手行・大手証券では、定期的かつシステム導入・大規模更改時に実施している先が多数を占めた（図表 27）。

[8] ハードウェアを構成する製品や、OS を含むソフトウェアのバージョンに関する情報など。

図表 27　脆弱性検査の実施状況



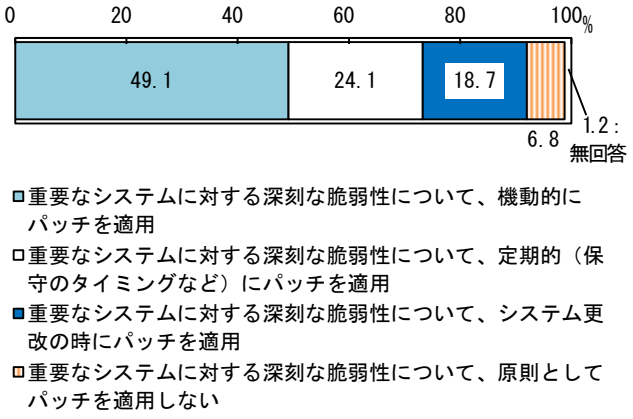
セキュリティ対策を適切に行っていると認識していても、自社に関係する脆弱性を見逃してしまうリスクは常に存在する。このため、脆弱性検査を適時適切に実施し、自社システムに対する外部からの侵入可能性や侵入後の攻撃可能性を点検することにより、脆弱性の早期の識別および適切な対応が可能となる。脆弱性検査は、システム設計・開発の過程で新たな脆弱性が生じやすいシステムの導入・大規模更改時だけでなく、隠れた脆弱性をあぶり出すためにも、定期的に実施することが望ましい。

脆弱性に対する修正プログラムの適用

（アンケート結果）

深刻な脆弱性に対し、約半数の先が機動的に修正プログラムを適用している。また、それ以外の多くの先は、定期的またはシステム更改のタイミングで修正プログラムを適用している（図表 28）。

図表 28　脆弱性に対する修正プログラム（パッチ）の適用



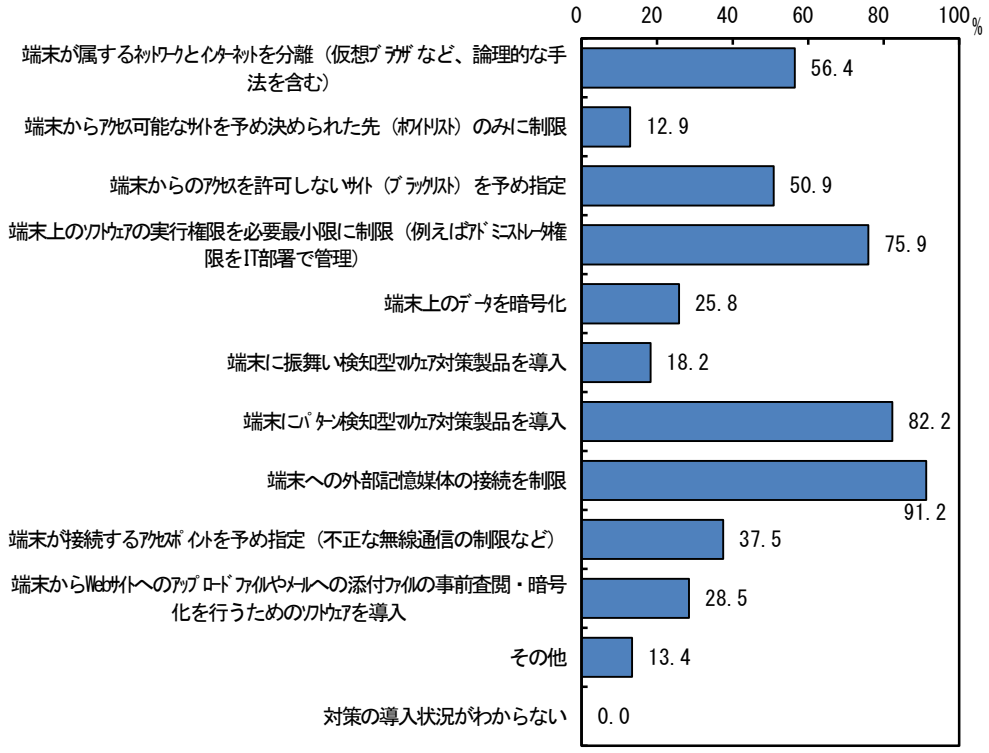
自社の重要システムに深刻な脆弱性が発見された場合には、その脆弱性を悪用した攻撃を受けた場合の影響度、修正プログラムを適用することによる他のシステムや業務への支障の有無などを考慮のうえ、できるだけ速やかに適切な調整と修正プログラムの適用を行う必要がある。自社の他システムや業務に影響が出るなど、やむを得ない理由で、修正プログラムの適用を速やかに行えない場合には、経営陣に報告するとともに、残余リスクを極小化したうえで適切な管理を実施する必要がある。なお、仮に、脆弱性が発見されたシステムについて、通常はインターネットに接続できない仕組みを導入していたとしても、多くの場合、サーバや外部記憶媒体を経由した外部とのデータの授受や、連携する業務委託先から自社システムへのアクセスなどの過程で、直接的または間接的に、情報が流出入するリスクが存在することに留意する必要がある。

端末へのマルウェア攻撃対策

（アンケート結果）

OA 端末[9]に関しては、全体の 6 割弱の先が、端末が属するネットワークとインターネットを分離することにより、マルウェアの侵入後に同ネットワークと外部との間で通信が確立するリスクの削減に努めている（図表 29）。

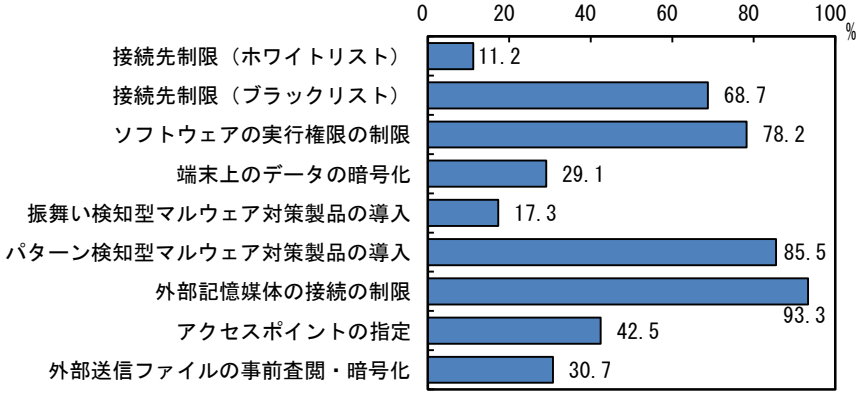
図表 29　OA 端末へのマルウェア攻撃対策（複数回答）



[9] ここでは、役職員が文書作成などに標準的に用いる端末を指す。

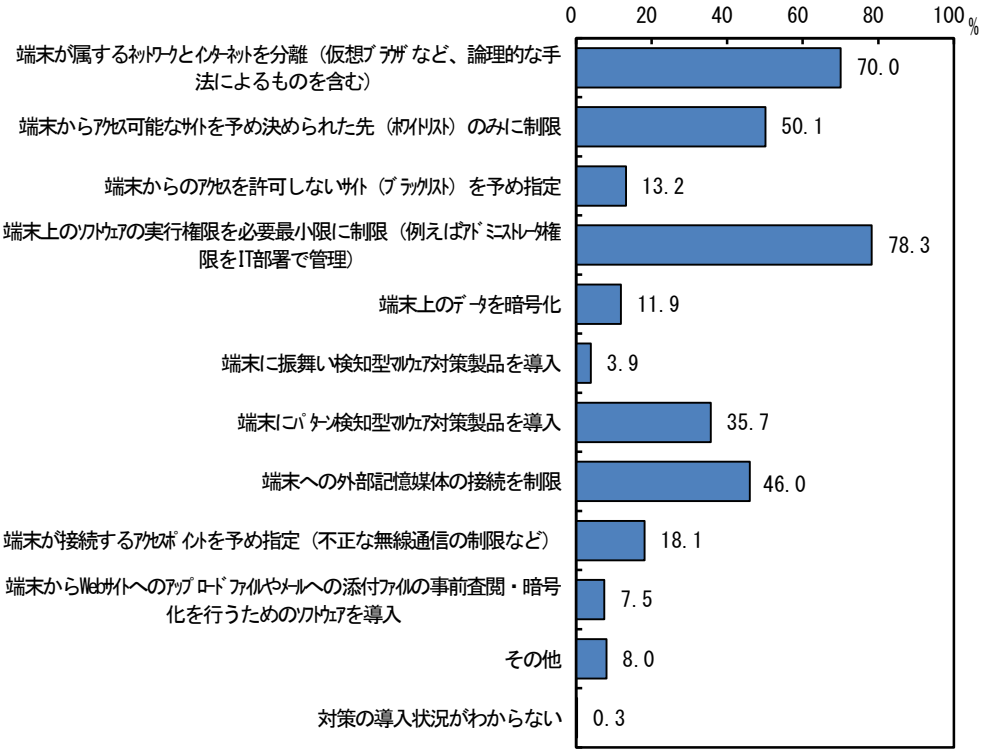
一方で、上述のネットワーク分離を行っていない先（ネットワーク未分離先）が採用している技術的対策[10]についてみると、「外部記憶媒体の接続を制限」、「パターン検知型マルウェア対策製品を導入」、「端末上のソフトウェアの実行権限を必要最小限に制限」、「端末からのアクセスを許可しないサイト（ブラックリスト）を予め指定」が上位に並んだ（図表 30）。

図表 30　ネットワーク未分離先における対策（OA 端末<複数回答>）



同様に、営業店端末[11]については、全体の 7 割の先が、端末が属するネットワークとインターネットを分離している（図表 31）。

図表 31　営業店端末へのマルウェア攻撃対策（複数回答）

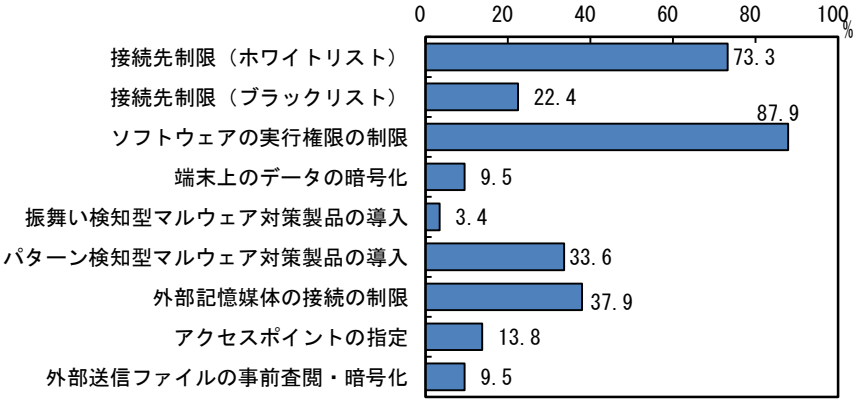


[10] 本アンケートでは、端末へのマルウェア攻撃対策として採用している「技術的対策」について質問した。わが国の金融機関は、通常、技術的対策を講じたうえで、「オペレーターと送信処理責任者による多段階承認」などの運用上の対策を講じている。

[11] ここでは、勘定系システムに接続する端末を指す。

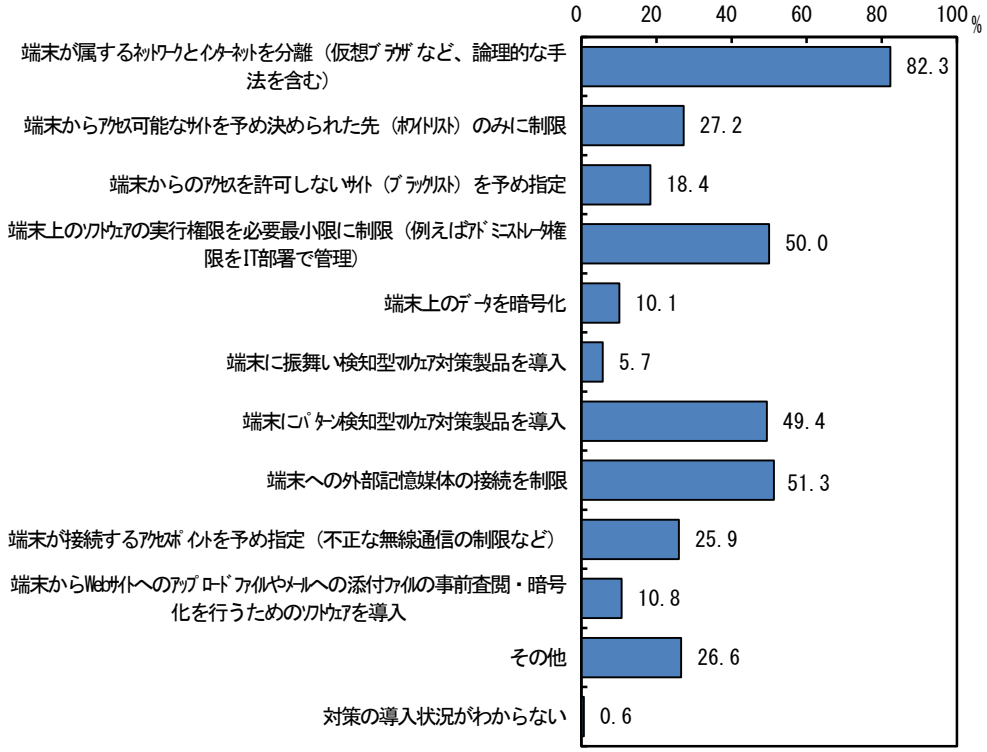
ネットワーク未分離先が採用している技術的対策をみると、「端末上のソフトウェアの実行権限を必要最小限に制限」、「端末からアクセス可能なサイトを予め決められた先（ホワイトリスト）のみに制限」といった対応を講じている先が多い（図表 32）。

図表 32　ネットワーク未分離先における対策（営業店端末〈複数回答〉）



また、SWIFT 端末[12]については、全体の 8 割超の先が、端末が属するネットワークとインターネットを分離している（図表 33）。

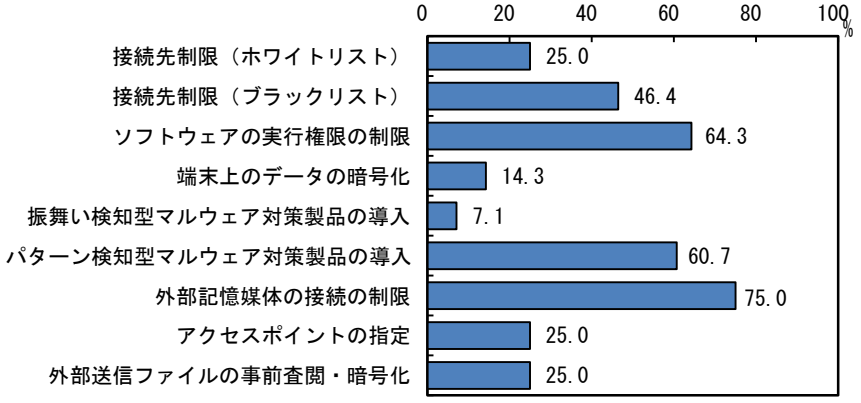
図表 33　SWIFT 端末へのマルウェア攻撃対策（複数回答）



[12] ここでは、SWIFT（クロスボーダー銀行取引におけるペーパーレス化を推進することを目的として設立された非営利協同組合）が提供する、利用組織間の取引に関するメッセージ伝送サービスに用いる端末を指す。

ネットワーク未分離先が採用している技術的対策をみると、「外部記憶媒体の接続を制限」、「端末上のソフトウェアの実行権限を必要最小限に制限」、「パターン検知型マルウェア対策製品を導入」といった対応を講じている（図表 34）。

図表 34　ネットワーク未分離先における対策（SWIFT 端末<複数回答>）



マルウェアは、インターネットメールや Web サイトの閲覧、外部記憶媒体などを通じて自社システムに侵入する。その後は、マルウェアの実行後に外部との通信を確立し、感染を拡大させ、重要情報を漏えいさせるものや、ネットワーク上でアクセス可能なデータやファイルを破壊・暗号化して利用不能にするものなど、マルウェアの種類により様々な攻撃を行う。

端末が属するネットワークとインターネットを分離することにより、マルウェアが自社システムに侵入したり、外部に情報を漏えいさせたりするリスクを軽減する効果が期待できる。ただし、金融機関が業務を効率的に行ううえで、外部との通信を完全に遮断することができない以上、ネットワークを分離した場合においても、マルウェアの侵入が生じる可能性が残るという点には、十分留意しておく必要がある。

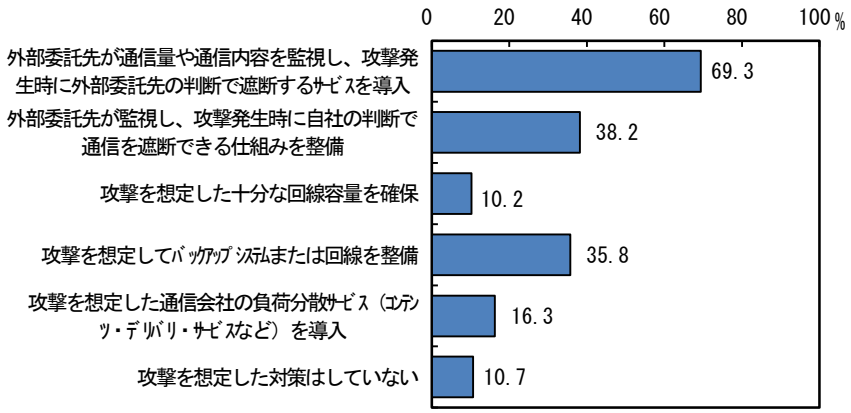
また、ネットワーク未分離先の場合、サイバー攻撃の手法が刻々と巧妙化していることを踏まえると、マルウェアの侵入を完全に防ぐことは困難であり、侵入を前提として被害を抑制するための総合的な対策を想定しておくことが必要である。その際には、対策の有効性が維持・確保されているかどうかを常に検証することが求められる。

ホームページへの DDoS 攻撃対策

（アンケート結果）

ホームページへの DoS 攻撃（DDoS 攻撃を含む）対策として、業務委託先がシステムの監視および通信遮断の判断を行うサービスを導入している先が多い[13]。また、大手行・大手証券では、バックアップシステム・回線の整備や負荷分散サービスの導入を行っている先も相応にみられた（図表 35）。

図表 35　ホームページへの DDoS 攻撃対策（複数回答）



DDoS 攻撃については、最近の攻撃規模の拡大傾向を踏まえれば、本格的な攻撃を受けた場合に完全に防御することは極めて困難と考えられる。このため、システムの利用が困難になった場合のコンティンジェンシープランを適切に整備する必要がある。このほか、業務継続上の重要性に応じて、攻撃の影響を緩和するためのサービスを導入することが求められる。

3．おわりに

わが国の金融セクターを巡るサイバー脅威の高まりを踏まえれば、金融機関がセキュリティ強化に向けた取り組みを続けていくことが、今後一段と重要になっていくものと考えられる。日本銀行としては、金融機関が自らのサイバーセキュリティに関する体制面や技術面での取り組みを進めていくうえで、本アンケート結果が活用されることを期待するとともに、金融機関とサイバーセキュリティに関する議論をさらに深めていく方針である。

[13] わが国の多くの金融機関のホームページは、IT ベンダーが構築と管理を受託し、銀行の内部システムとは切り離したかたちで、インターネットとの接続を専用に行うシステムとして運用されている。